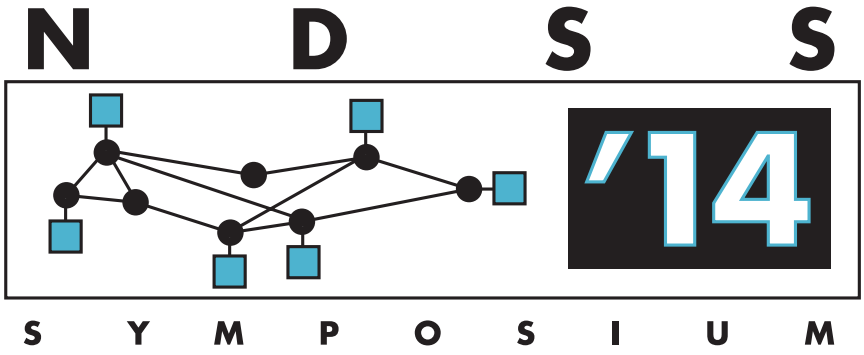
Proceedings

2014

Network and Distributed System Security Symposium



Proceedings

2014

Network and Distributed System Security Symposium

February 23 – 26, 2014

San Diego, California

Sponsored by the
Internet Society

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108

Address your correspondence to: Senior Events Manager, Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, Virginia 20190-5108, U.S.A., tel. +1 703 439 2120, fax +1 703 326 9881, ndss@isoc.org.

The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.

ISBN Number (Digital Format) 1-891562-35-5

Additional copies may be ordered from:

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Proceedings of the 2014 Network and Distributed System Security Symposium

Table of Contents

HYBRID-BRIDGE: Efficiently Bridging the Semantic Gap in Virtual Memory Introspection via Decoupled Execution and Training Memoization
A. Saberi, Y. Fu, Z. Lin

SESSION 3: Security of Mobile Devices I

Screenmilker: How to Milk Your Android Screen for Secrets
C. Lin, H. Li, X. Zhou, X.F. Wang

AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable
S. Dey, N. Roy, W. Xu, R.R. Choudhury, S. Nelakuditi

Smartphones as Practical and Secure Location Verification Tokens for Payments
C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, S. Čapkun

Breaking and Fixing Origin-Based Access Control in Hybrid Web/Mobile Application Frameworks
M. Georgiev, S. Jana, V. Shmatikov

Inside Job: Understanding and Mitigating the Threat of External Device Mis-Bonding on Android
M. Naveed, X. Zhou, S. Demetriou, X.F. Wang, C.A. Gunter

SESSION 4: Web Security

DSpin: Detecting Automatically Spun Content on the Web
Q. Zhang, D.Y. Wang, G.M. Voelker

Toward Black-Box Detection of Logic Flaws in Web Applications
G. Pellegrino, D. Balzarotti

Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud
A. Birgisson, J.G. Politz, U. Erlingsson, A. Taly, M. Vrable, M. Lentczner

Detecting Logic Vulnerabilities in E-commerce Applications
F. Sun, L. Xu, Z. Su

Simulation of Built-in PHP Features for Precise Static Code Analysis
J. Dahse, T. Holz

SESSION 5: Privacy

Efficient Private File Retrieval by Combining ORAM and PIR
T. Mayberry, E.-O. Blass, A.H. Chan

Privacy through Pseudonymity in Mobile Telephony Systems
M. Arapinis, L.I. Mancini, E. Ritter, M. Ryan

Privacy-Preserving Distributed Stream Monitoring
A. Friedman, I. Sharfman, D. Keren, A. Schuster

The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network
R. Jansen, F. Tschorsch, A. Johnson, B. Scheuermann

Selling off Privacy at Auction
L. Olejnik, M.-D. Tran, C. Castelluccia

SESSION 6: Authentication and Identity I

The Tangled Web of Password Reuse
A. Das, J. Bonneau, M. Caesar, N. Borisov, X.F. Wang

On the Semantic Patterns of Passwords and their Security Impact
R. Veras, C. Collins, J. Thorpe

From *Very Weak* to *Very Strong*: Analyzing Password-Strength Meters
X. de Carné de Carnavalet, M. Mannan

SESSION 7: Crypto I

Copker: Computing with Private Keys without RAM
L. Guan, J. Lin, B. Luo, J. Jing

Practical Dynamic Searchable Encryption with Small Leakage
E. Stefanov, C. Papamanthou, E. Shi

Decentralized Anonymous Credentials
C. Garman, M. Green, I. Miers

Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation
D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, M. Steiner

SESSION 8: Authentication and Identity II

Authentication Using Pulse-Response Biometrics
K.B. Rasmussen, M. Roeschlin, I. Martinovic, G. Tsudik

Hardening Persona – Improving Federated Web Login
M. Dietz, D.S. Wallach

Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices
M. Shirvanian, S. Jarecki, N. Saxena, N. Nathan

Leveraging USB to Establish Host Identity Using Commodity Devices
A. Bates, R. Leonard, H. Pruse, D. Lowd, K.R.B. Butler

SESSION 9: New Applications, Attacks, and Security Economics

PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces
R. Templeman, M. Korayem, D. Crandall, A. Kapadia

Auditable Version Control Systems
B. Chen, R. Curtmola

Power Attack: An Increasing Threat to Data Centers
Z. Xu, H. Wang, Z. Xu, X. Wang

Scambaiter: Understanding Targeted Nigerian Scams on Craigslist
Y. Park, J. Jones, D. McCoy, E. Shi, M. Jakobsson

Botcoin: Monetizing Stolen Cycles
D.Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A.C. Snoeren, K. Levchenko

SESSION 10: Security of Mobile Devices II

A Machine-learning Approach for Classifying and Categorizing Android Sources and Sinks
S. Rasthofer, S. Arzt, E. Bodden

AirBag: Boosting Smartphone Resistance to Malware Infection
C. Wu, Y. Zhou, K. Patel, Z. Liang, X. Jiang

SMV-HUNTER: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps
D. Sounthiraraj, J. Sahs, G. Greenwood, Z. Lin, L. Khan

AppSealer: Automatic Generation of Vulnerability-Specific Patches for Preventing Component Hijacking Attacks in Android Applications
M. Zhang, H. Yin

Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications
S. Poeplau, Y. Fratantonio, A. Bianchi, C. Kruegel, G. Vigna

SESSION 11: Malware

Nazca: Detecting Malware Distribution in Large-Scale Networks
L. Invernizzi, S. Miskovic, R. Torres, S. Saha, S.-J. Lee, M. Mellia, C. Kruegel, G. Vigna

Persistent Data-only Malware: Function Hooks without Code
S. Vogl, J. Pfoh, T. Kittel, C. Eckert

Drebin: Effective and Explainable Detection of Android Malware in Your Pocket
D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, K. Rieck

Gyrus: A Framework for User-Intent Monitoring of Text-Based Networked Applications
Y. Jang, S.P. Chung, B.D. Payne, W. Lee

Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings
A. Neupane, N. Saxena, K. Kuruvilla, M. Georgescu, R. Kana

SESSION 12: Crypto II

Web PKI: Closing the Gap between Guidelines and Practices
A. Delignat-Lavaud, M. Abadi, A. Birrell, I. Mironov, T. Wobber, Y. Xie

Enhanced Certificate Transparency and End-to-end Encrypted Mail
M.D. Ryan

Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems
M. Schulz, A. Loch, M. Hollick

Practical Issues with TLS Client Certificate Authentication
A. Parsovs

General Chair's Message

It is my pleasure to welcome you all back to the beautiful Catamaran Resort Hotel and Spa on Mission Bay in San Diego for the Internet Society's Network and Distributed System Security Symposium (NDSS'14).

I would like to thank the Catamaran Resort for providing such an excellent venue for us over the years and for this, our 21st year. From our very first workshop and continuing today, NDSS has striven to maintain the superior quality of our technical program. Our research domain continues to emphasize practical applications of security based on solid theoretical foundations. The program stretches from canonical to current, and includes both the theoretical and the pressing needs. This scope, along with a willingness to consider potentially controversial or unusual research, is the essential beauty of NDSS.

This year we have added optional SENT and USEC full day Workshops (Security of Emerging Network Technologies and Usable Security) on Sunday. These will bring together academic and industry researchers to discuss security problems, challenges, and potential security solutions of emerging networking technologies such as Software Defined Networks, Named-Data-Networking and Cellular networks.

The main program for this year packs a lot into three days and includes 12 sessions and 55 original research papers. They cover a variety of current topics such as issues with password reuse, authentication methods, biometrics, cloud computing, distributed systems and networks, web security and privacy, intrusion detection and attack analysis, anonymity, and more. Our keynote speaker this year is Christopher Hadnagy, Chief Human Hacker of Social-Engineer, Inc. He will talk about "Hacking the Human".

Although the symposium revolves around the technical presentations, there is far more to the experience. Take advantage of the hall track, the reception, the lunches, and the Tuesday banquet to meet new colleagues. This year we have added a poster session to the reception. Please check them out. Participate in the discussions. And finally, remember to save some time to take advantage of our fantastic geographic location.

This symposium is possible only through the hard work of many people. I would like to thank the NDSS steering group for charting a course for the conference that keeps its focus current, relevant, and practical. David Balenson, one of NDSS's original steering group members rejoins us this year as Publications Chair and has skillfully assembled the Proceedings. Kevin Craemer again has done a wonderful job of finding sponsors and helping plan and publicize the conference and Terry Weigler, as always has done a fantastic job dealing with each and every one of you for Registration. This meeting is as enjoyable and as successful as it is because of the efforts of these people -- it is no exaggeration to say that NDSS simply would not happen without each of their contributions.

The quality of this conference directly depends upon the quality of the papers accepted. The program committee, under the direction of Program Chair Lujo Bauer of Carnegie Mellon University, has done a fantastic job and has selected an extraordinary set of papers. I thank Lujo and the entire program committee for their expertise, hard work, and dedication. I also want to thank Li Erran Li from Bell Labs, Alcatel-Lucent and Adrian Perrig for organizing and chairing the SENT workshop and Matthew Smith of Leibniz University Hannover and David Wagner of UC Berkeley for the organizing and chairing of the USEC workshop. Lastly, I also thank the authors who submitted papers and the speakers who are present; YOU are the core of this symposium.

I am also grateful for our sponsors, as it would be impossible to hold such an event without them. Our sponsors are the Internet Society for overall sponsorship, Cisco Systems for Gold Sponsorship; Afilias, Qualcomm, the San Diego Supercomputer Center @ UCSD (SDSC), and Samsung Knox for Silver sponsorship; Research at Google, Internet2, and Microsoft Research for Bronze sponsorships, and IEEE Security and Privacy Magazine as our media sponsor. The conference is organized by the Internet Society, in cooperation with USENIX.

I would also like to thank my organization, the San Diego Supercomputer Center at the University of California San Diego, for supporting my involvement with this symposium for the last twenty-one years. Finally, I want all of you to know that I view it as a great honor to chair this conference, one where the attendees and speakers are some of the finest minds in computer network security.

Thomas Hutton
General Chair, NDSS'14
San Diego Supercomputer Center
University of California, San Diego

Program Chair's Message

It is my great pleasure to welcome you to the 21st Annual Network & Distributed System Security Symposium (NDSS 2014), held at the Catamaran Resort Hotel and Spa in San Diego, CA, United States on February 23-26, 2014. NDSS fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of network and distributed systems security technologies.

This year NDSS received 290 valid submissions (i.e., not counting papers that clearly violated the submission guidelines). Submissions were evaluated on the basis of their technical quality, novelty, and significance. Papers went through three rounds of review, and, new this year, authors were given the chance to see and respond to reviews after the second round. Reviewing culminated in a one-and-a-half-day in-person program committee meeting, at which 55 papers (approximately 19%) were selected to appear at NDSS.

Organizing a conference as large as NDSS is a substantial endeavor, and I'd like to extend my sincere thanks to everyone who contributed his or her time and effort. I'd also like to specifically thank a few individuals who made particular contributions to NDSS 2014. Kevin Craemer handled most of the logistics of organizing the conference, as well as the more challenging task of shepherding a new program chair. Engin Kirda served as the shadow chair; my job was much easier because he was there to catch any oversights. Thanks chiefly to the efforts and persistence of David Balenson, the Publications Chair, NDSS 2014 proceedings and papers have been assigned digital object identifiers (DOIs), enabling easier search and indexing. I'd also like to thank everyone who served on the program committee; it was my pleasure and honor to have worked with you to put together the program for NDSS 2014. Also crucial to the success of NDSS are the authors who submitted papers---thank you!---and the attendees. Welcome to NDSS, and I hope you find the program informative and stimulating.

Lujo Bauer
Program Chair, NDSS'14
Carnegie Mellon University

Program Committee

Lujo Bauer (Chair), Carnegie Mellon University, USA

Michael Bailey, University of Michigan, USA

Dirk Balfanz, Google, USA

Davide Balzarotti, EURECOM, France

Juan Caballero, IMDEA, Spain

Srdjan Capkun, ETH Zurich, Switzerland

Yan Chen, Northwestern University, USA

Nicolas Christin, Carnegie Mellon University, USA

Mihai Christodorescu, Qualcomm, USA

William Enck, NC State University, USA

Nick Feamster, Georgia Tech, USA

Vinod Ganapathy, Rutgers University, USA

Guofei Gu, Texas A&M University, USA

Krishna P. Gummadi, MPI-SWS, Germany

Thorsten Holz, Ruhr-University Bochum, Germany

Nick Hopper, University of Minnesota, USA

Trent Jaeger, Penn State, USA

Xuxian Jiang, NC State University, USA

Chris Kanich, University of Illinois at Chicago, USA

Apu Kapadia, Indiana University, USA

Engin Kirda, Northeastern University, USA

Christian Kreibich, ICSI, USA

Brian Levine, UMass Amherst, USA

Zhenkai Liang, National University of Singapore, Singapore

Jay Lorch, Microsoft Research, USA

Long Lu, Stony Brook University, USA

Morley Mao, University of Michigan, USA

Jonathan McCune, Google, USA

Prateek Mittal, UC Berkeley, USA

Phil Porras, SRI International, USA

Michael Reiter, UNC Chapel Hill, USA

Thomas Ristenpart, University of Wisconsin, USA

Ahmad-Reza Sadeghi, TU Darmstadt, Germany

Vyas Sekar, Stony Brook University, USA

Asia Slowinska, Vrije Universiteit Amsterdam, The Netherlands

Robin Sommer, ICSI/LBNL, USA

Patrick Tague, Carnegie Mellon University, USA

Gang Tan, Lehigh University, USA

Patrick Traynor, Georgia Institute of Technology, USA

David Wagner, UC Berkeley, USA

Helen Wang, Microsoft Research, USA

XiaoFeng Wang, Indiana University, USA

Matthew Wright, University of Texas at Arlington, USA

Yinglian Xie, Microsoft Research, USA

Dongyan Xu, Purdue University, USA

Wenyuan Xu, University of South Carolina, USA

Ting-Fang Yen, RSA Labs, USA

Organizing Committee

General Chair and Local Arrangements Chair

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego
hutton@ucsd.edu

Program Chair

Lujo Bauer
Carnegie Mellon University
lbauer@cmu.edu

Publications Chair and Historian

David Balenson
SRI International
david.balenson@sri.com

Conference Coordinator, Publicity Chair, and Sponsorship Coordinator

Kevin Craemer
Internet Society
craemer@isoc.org

Steering Group

Co-Chairs

Thomas Hutton
San Diego Super Computer Center
University of California, San Diego

Leslie Daigle
Chief Internet Technology Officer
Internet Society

Administrative Coordinator

Kevin Craemer
Internet Society

Steering Group Members

Lujo Bauer
Carnegie Mellon University

Deb Frincke
National Security Agency

Yongdae Kim
Korea Advanced Institute of Science and Technology

Engin Kirda
Northeastern University

Tadayoshi (Yoshi) Kohno
University of Washington

David Molnar
Microsoft Research

Clifford Neuman
University of Southern California

Paul Syverson
Naval Research Lab

Doug Szajda
University of Richmond

Giovanni Vigna
University of California, Santa Barbara

Helen Wang
Microsoft Research